PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-258972
(43)Date of publication of application : 13.09.2002

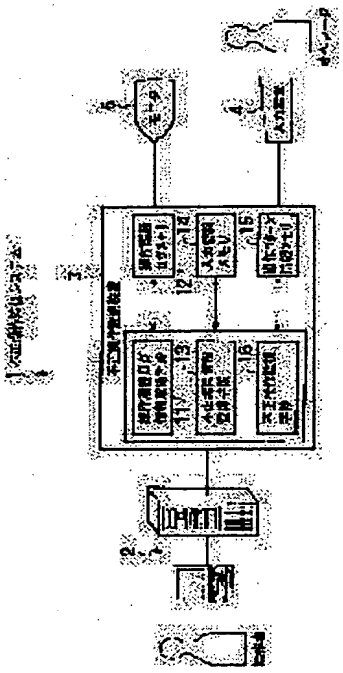
(51)Int.Cl. G06F 1/00

(21)Application number : 2001-054823
(22)Date of filing : 28.02.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : ISHIKAWA KATSUYOSHI

(54) ILLEGAL OPERATION MONITOR DEVICE AND ITS PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an illegal operation monitor device capable of monitoring any illegal input and operation in real time by always monitoring the operation history log of a computer system to be monitored.
SOLUTION: This illegal operation monitor device 3 is provided with an operation history log information acquiring means 11 for acquiring operation history log information from a computer system 2 to be monitored, an operation history log memory 12 for storing the operation history log information, an illegality discovery information registering means 13 for registering illegal discovery information for discovering any illegal operation, an input information memory 14 for storing input information such as a key input interval or an input alarm value being the illegality discovery information, an operation pattern information memory 15 for storing operation pattern information being the illegality discovery information, and an illegal operation monitoring means 16 for monitoring the illegal operation by comparing the illegality discovery information with operation history log information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－258972
（P2002－258972A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全６頁）

(21)出願番号　特願2001－54823(P2001－54823)

(22)出願日　平成13年２月28日(2001.2.28)

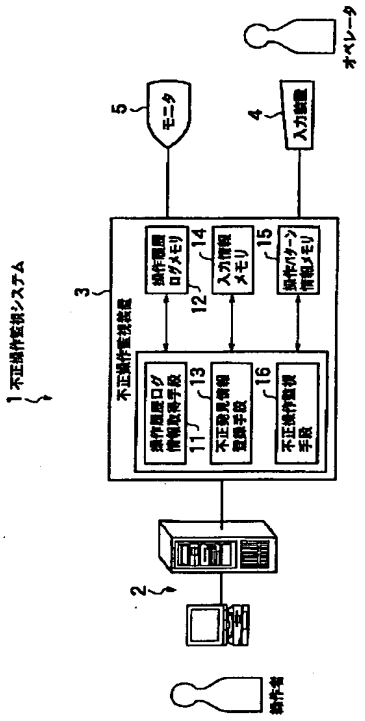
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号

(72)発明者　石川　勝義
東京都府中市東芝町１番地　株式会社東芝府中事業所内

(74)代理人　100083806
弁理士　三好　秀和　（外７名）

(54)【発明の名称】　不正操作監視装置及び不正操作監視プログラム

(57)【要約】
【課題】　監視対象コンピュータシステムの操作履歴ログを常に監視することによって、不正入力・操作をリアルタイムで監視することのできる不正操作監視装置を提供する。
【解決手段】　本発明の不正操作監視装置３は、監視対象コンピュータシステム２から操作履歴ログ情報を取得する操作履歴ログ情報取得手段１１と、この操作履歴ログ情報を記憶する操作履歴ログメモリ１２と、不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録手段１３と、不正発見情報であるキー入力間隔や入力警告値などの入力情報を記憶する入力情報メモリ１４と、不正発見情報である操作パターン情報を記憶する操作パターン情報メモリ１５と、不正発見情報と操作履歴ログ情報とを比較して不正操作を監視する不正操作監視手段１６とを含んでいる。



1

【特許請求の範囲】

【請求項１】　監視対象コンピュータシステムが操作された履歴に関する操作履歴ログ情報を取得する操作履歴ログ情報取得手段と、

前記監視対象コンピュータシステムへの不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録手段と、

この不正発見情報登録手段で登録された前記不正発見情報と、前記操作履歴ログ情報とを比較して前記監視対象コンピュータシステムへの不正操作を発見する不正操作監視手段とを含むことを特徴とする不正操作監視装置。

【請求項２】　前記不正発見情報は、入力項目を入力するときの最長時間と最短時間との時間間隔によって設定されたキー入力間隔であることを特徴とする請求項１に記載の不正操作監視装置。

【請求項３】　前記不正発見情報は、入力内容の数値の最大値と最小値とに基づいて設定された入力警告値であることを特徴とする請求項１または２に記載の不正操作監視装置。

【請求項４】　前記不正発見情報は、入力項目が入力される順序によって設定された入力パターンであることを特徴とする請求項１、２または３に記載の不正操作監視装置。

【請求項５】　監視対象コンピュータシステムが操作された履歴に関する操作履歴ログ情報を取得する操作履歴ログ情報取得処理と、

前記監視対象コンピュータシステムへの不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録処理と、

この不正発見情報登録処理で登録された前記不正発見情報と、前記操作履歴ログ情報とを比較して前記監視対象コンピュータシステムへの不正操作を発見する不正操作監視処理とを含むことを特徴とする不正操作監視プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステムへの不正操作を監視する不正操作監視装置に係り、特に監視対象コンピュータシステムの操作履歴ログを常に監視することによって、不正操作が行われた際にリアルタイムで発見することのできる不正操作監視装置に関する。

【０００２】

【従来の技術】従来からコンピュータシステムにおける不正入力や不正操作を発見、防止するために、さまざまな方法が取られてきた。その方法の１つとして入力・操作の履歴を操作履歴ログとして保存しておき、後で不正の分析に役立てる方法があった。この方法では、不正入力や不正操作が発覚すると、操作履歴ログの内容から誰が何を入力・操作したかを分析して不正者をつきとめていた。

2

【０００３】

【発明が解決しようとする課題】しかしながら、上述した方法では、操作履歴ログをあくまで不正発覚後に不正者をつきとめるために使用するものであり、不正な入力や操作が行われた際には操作履歴ログは活用されていなかった。

【０００４】したがって、従来の方法では不正入力・操作が行われた際に、不正を発見することができないという問題点があった。

【０００５】また、従来の方法では、操作者のＩＤとパスワードが盗まれてしまうと、不正な入力・操作は正常に処理されることになり、不正を発見することができないという問題点もあった。

【０００６】本発明は上記事情に鑑みてなされたものであり、その目的は、監視対象コンピュータシステムの操作履歴ログを常に監視することによって、不正入力・操作をリアルタイムで監視することのできる不正操作監視装置を提供することにある。

【０００７】

【課題を解決するための手段】上記目的を達成するために、請求項１に記載の発明である不正操作監視装置は、監視対象コンピュータシステムが操作された履歴に関する操作履歴ログ情報を取得する操作履歴ログ情報取得手段と、前記監視対象コンピュータシステムへの不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録手段と、この不正発見情報登録手段で登録された前記不正発見情報と、前記操作履歴ログ情報とを比較して前記監視対象コンピュータシステムへの不正操作を発見する不正操作監視手段とを含むことを特徴とする。

【０００８】この請求項１の発明によれば、監視対象コンピュータシステムから操作履歴ログ情報を取得して常に監視するので、不正な操作者による不正入力をリアルタイムで発見することができる。

【０００９】請求項２に記載の発明である不正操作監視装置の不正発見情報は、入力項目を入力するときの最長時間と最短時間との時間間隔によって設定されたキー入力間隔であることを特徴とする。

【００１０】この請求項２の発明によれば、キー入力間隔によって不正操作を監視するので、操作者ＩＤやパスワードが盗まれた場合でも不正操作を発見することができる。

【００１１】請求項３に記載の発明である不正操作監視装置の不正発見情報は、入力内容の数値の最大値と最小値とに基づいて設定された入力警告値であることを特徴とする。

【００１２】この請求項３の発明によれば、入力警告値によって不正操作を監視するので、操作者ＩＤやパスワードが盗まれた場合でも不正操作を発見することができ

る。

【００１３】請求項４に記載の発明である不正操作監視装置の不正発見情報は、入力項目が入力される順序によって設定された入力パターンであることを特徴とする。

【００１４】この請求項４の発明によれば、操作パターン情報によって不正操作を監視するので、操作者ＩＤやパスワードが盗まれた場合でも不正操作を発見することができる。

【００１５】請求項５に記載の発明である不正操作監視プログラムは、監視対象コンピュータシステムが操作された履歴に関する操作履歴ログ情報を取得する操作履歴ログ情報取得処理と、前記監視対象コンピュータシステムへの不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録処理と、この不正発見情報登録処理で登録された前記不正発見情報と、前記操作履歴ログ情報とを比較して前記監視対象コンピュータシステムへの不正操作を発見する不正操作監視処理とを含むことを特徴とする。

【００１６】この請求項５の発明によれば、監視対象コンピュータシステムから操作履歴ログ情報を取得して常に監視するので、不正な操作者による不正入力をリアルタイムで発見することができる。

【００１７】

【発明の実施の形態】以下、本実施形態に係る不正操作監視システムの構成を図１に基づいて説明する。

【００１８】図１に示すように、不正操作監視システム１は、不正操作が行われているか否かを監視する対象である監視対象コンピュータシステム２と、この監視対象コンピュータシステム２から操作履歴に関する操作履歴ログ情報を取得して不正操作の監視処理を行う不正操作監視装置３と、この不正操作監視装置３に対してオペレータが入力を行うための入力装置４と、不正操作監視装置３で出力された処理結果や警告を表示するモニタ５とから構成されている。

【００１９】ここで、不正操作監視装置３は、監視対象コンピュータシステム２が操作された履歴である操作履歴ログ情報を取得する操作履歴ログ情報取得手段１１と、この操作履歴ログ情報を記憶する操作履歴ログメモリ１２と、監視対象コンピュータシステム２への不正操作を発見するための情報である不正発見情報を登録する不正発見情報登録手段１３と、キー入力間隔や入力警告値などの不正を発見するための入力情報を記憶する入力情報メモリ１４と、監視対象コンピュータシステム２に対する入力項目の入力順序である操作パターンを記憶する操作パターン情報メモリ１５と、キー入力間隔や入力項目の数値、操作パターンなどの不正発見情報と操作履歴ログ情報とを比較して監視対象コンピュータシステム２への不正操作を監視する不正操作監視手段１６とを含んでいる。なお、不正操作監視装置３は、各種の処理を行うためのＣＰＵと、この処理の命令を記憶する記憶手段とを含む通常のコンピュータシステムによって構成されている。

【００２０】次に、図２のフローチャートに基づいて本実施形態に係る不正操作監視システム１による不正発見情報の登録処理について説明する。ここでは、不正発見情報として、キー入力間隔、入力警告値及び操作パターン情報を登録する場合を説明する。

【００２１】まず、不正操作監視装置３は、監視対象コンピュータシステム２を操作する操作者の操作内容や入力内容に関する操作履歴ログ情報を取得する（Ｓ２０１）。この操作履歴ログ情報は、図３に示すように操作者ＩＤ、操作日時、操作画面、入力項目、入力内容、キー入力時間などの情報が含まれている。

【００２２】そして、不正操作監視装置３は操作履歴ログ情報を取得すると、操作履歴ログメモリ１２に書き込む（Ｓ２０２）。

【００２３】次に、不正操作監視装置３は、不正を発見するための情報である不正発見情報の登録を行うが、ここで不正操作監視装置３を操作するオペレータが不正発見情報を自動登録するか直接登録するかを選択する（Ｓ２０３）。

【００２４】そして、オペレータが自動登録を選択した場合には、不正操作監視装置３は操作履歴ログメモリ１２に書き込まれている操作履歴ログ情報を取り込み（Ｓ２０４）、まずキー入力時間の最大値と最小値を各入力内容毎に求め、その最大値と最小値との時間間隔をキー入力間隔として設定し、入力情報メモリ１４に書き込む（Ｓ２０５）。

【００２５】さらに、入力内容についても、払出額や受入額などについては最大値と最小値を求め、その最大値と最小値の範囲を入力警告値として設定し、入力情報メモリ１４に書き込む（Ｓ２０６）。この入力情報メモリ１４に書き込まれた情報の一例を図４に示す。

【００２６】次に、不正操作監視装置３は操作履歴ログ情報から入力項目などを入力したときの操作順序を求め、その操作順序を操作パターン情報として設定し、操作パターン情報メモリ１５に書き込む（Ｓ２０７）。この操作パターン情報の一例を図５に示す。図５に示すように、操作パターン情報には各操作者ＩＤ毎に操作した内容が操作順に記録されている。

【００２７】こうして、キー入力間隔、入力警告値及び操作パターン情報とがそれぞれ設定されると、自動登録による不正発見情報の登録処理は終了する。

【００２８】また、ステップＳ２０３において、自動登録が選択されなかった場合には、不正操作監視装置３を操作するオペレータによる直接登録が行われる。

【００２９】この直接登録では、オペレータがまず任意に設定したキー入力間隔を入力し（Ｓ２０８）、同様に入力警告値についてもオペレータが入力して（Ｓ２０９）入力情報メモリ１４に書き込まれる。

【００３０】さらに、操作パターン情報についてもオペレータが任意に設定して入力し（Ｓ２１０）、操作パターン情報メモリ１５に書き込まれる。

【００３１】こうして、キー入力間隔、入力警告値及び操作パターン情報とがそれぞれオペレータによって入力されると、直接登録による不正発見情報の登録処理は終了する。

【００３２】次に、図６のフローチャートに基づいて、キー入力間隔による不正操作の監視処理について説明する。

【００３３】まず、不正操作監視装置３は、入力情報メモリ１４からキー入力間隔を取り込み（Ｓ６０１）、さらに操作履歴ログメモリ１２からキー入力時間を取り込む（Ｓ６０２）。

【００３４】そして、取り込まれたキー入力時間がキー入力間隔の範囲内にあるか否かを比較し（Ｓ６０３）、キー入力時間がキー入力間隔の範囲内にないときには不正な操作者による入力であると判断して警告メッセージをモニタ５に出力するなどして（Ｓ６０４）、オペレータに不正操作の警告を発してキー入力間隔による不正操作の監視処理は終了する。

【００３５】また、ステップＳ６０３において、キー入力時間がキー入力間隔の範囲内にあるときには正当な操作者による入力であると判断してキー入力間隔による不正操作の監視処理は終了する。

【００３６】同様に、図７のフローチャートに基づいて、入力警告値による不正操作の監視処理について説明する。

【００３７】まず、不正操作監視装置３は、入力情報メモリ１４から入力警告値を取り込み（Ｓ７０１）、さらに操作履歴ログメモリ１２から入力項目に対する入力内容を取り込む（Ｓ７０２）。

【００３８】そして、取り込まれた入力内容の払出額などの数値が入力警告値の範囲内にあるか否かを比較し（Ｓ７０３）、入力内容の数値が入力警告値の範囲内にないときには不正な操作者による入力であると判断して警告メッセージをモニタ５に出力するなどして（Ｓ７０４）、オペレータに不正操作の警告を発して入力警告値による不正操作の監視処理は終了する。

【００３９】また、ステップＳ７０３において、入力内容の数値が入力警告値の範囲内にあるときには正当な操作者による入力であると判断して入力警告値による不正操作の監視処理は終了する。

【００４０】次に、図８のフローチャートに基づいて、操作パターン情報による不正操作の監視処理について説明する。

【００４１】まず、不正操作監視装置３は、操作パターン情報メモリ１５から操作パターン情報を取り込み（Ｓ８０１）、さらに操作履歴ログメモリ１２から入力項目と入力内容を取り込む（Ｓ８０２）。

【００４２】そして、操作履歴ログメモリ１２から取り込まれた入力内容の操作順序が操作パターンの順序と異なるか否かを比較し（Ｓ８０３）、入力内容の操作順序が異なるときには不正な操作者による入力であると判断して警告メッセージをモニタ５に出力するなどして（Ｓ８０４）、オペレータに不正操作の警告を発して操作パターンによる不正操作の監視処理は終了する。ただし、このとき操作順序が１つでも異なれば警告を発するように設定してもよいし、また任意に設定した数までは操作順序が異なっても警告を発しないように設定してもよい。

【００４３】また、ステップＳ８０３において、入力内容の操作順序が操作パターンの順序と一致するときには正当な操作者による入力であると判断して操作パターン情報による不正操作の監視処理は終了する。

【００４４】このように、本実施形態の不正操作監視装置３は、監視対象コンピュータシステム２の操作履歴ログ情報を取得して常に監視することによって、リアルタイムで不正な操作者による不正な入力や操作を発見することができる。

【００４５】さらに、キー入力間隔や入力警告値、操作パターンによって不正操作を監視するので、操作者ＩＤやパスワードが盗まれた場合でも不正な操作を発見することができる。

【００４６】

【発明の効果】以上説明したように、本発明の不正操作監視装置によれば、監視対象コンピュータシステムへの不正入力や不正操作を、リアルタイムで監視することができる。

【図面の簡単な説明】

【図１】本発明による不正操作監視システムの一実施形態の構成を示すブロック図である。

【図２】図１に示す不正操作監視システムにおける不正発見情報の登録処理を説明するためのフローチャートである。

【図３】操作履歴ログ情報の一例を示す図である。

【図４】入力情報の一例を示す図である。

【図５】操作パターン情報の一例を示す図である。

【図６】キー入力間隔による不正操作の監視処理を説明するためのフローチャートである。

【図７】入力警告値による不正操作の監視処理を説明するためのフローチャートである。

【図８】操作パターン情報による不正操作の監視処理を説明するためのフローチャートである。

【符号の説明】

１　不正操作監視システム
２　監視対象コンピュータシステム
３　不正操作監視装置
４　入力装置
５　モニタ

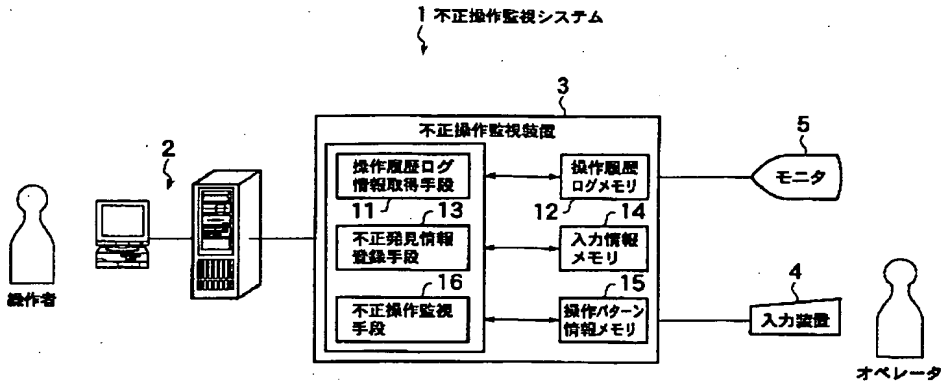
7

１１　操作履歴ログ情報取得手段
１２　操作履歴ログメモリ
１３　不正発見情報登録手段

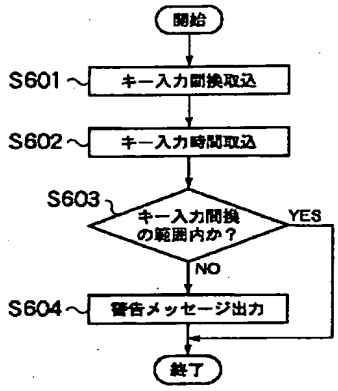
8

＊１４　入力情報メモリ
１５　操作パターン情報メモリ
＊　１６　不正操作監視手段

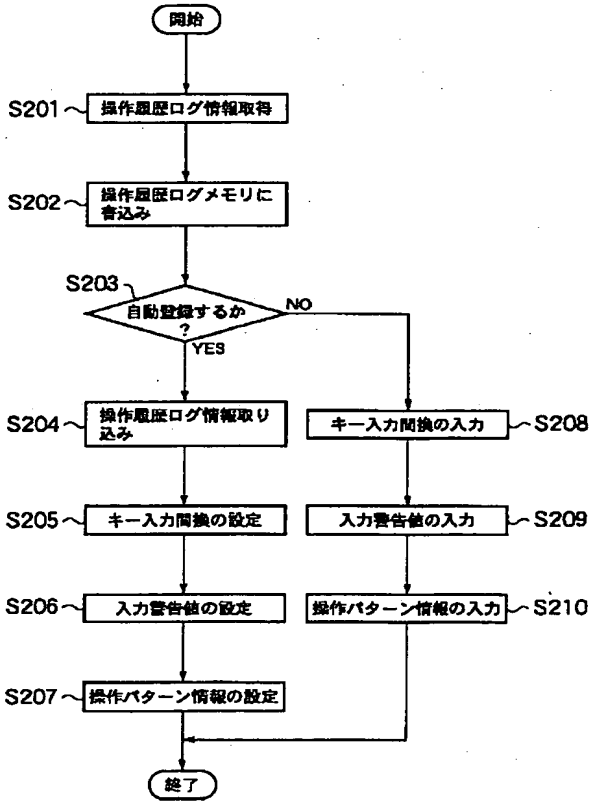
【図１】



【図６】



【図２】



【図４】

操作者ID	操作画面	入力項目	キー入力間隔	入力警告値
AAA	預金払出	口座番号	0.2秒～0.6秒	-
		氏名	0.2秒～0.4秒	-
		性別	0.3秒～0.4秒	-
		年齢	0.4秒～0.5秒	-
		払出額	0.4秒～0.8秒	0～50,000
AAA	預金受入	口座番号	0.3秒～0.4秒	-
：	：	：	：	：
		受入額	0.2秒～0.8秒	0～10,000
BBB	預金払出	払出額	1.0秒～2.0秒	0～10,000
：	：	：	：	：

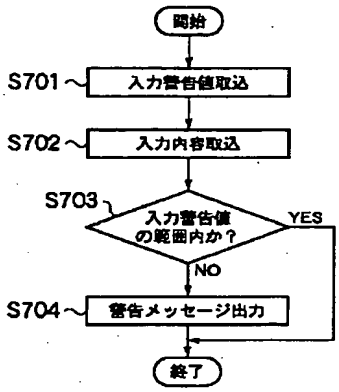
【図５】

操作者ID	操作パターン
AAA	預金払出画面入力ボタン押下→預金払出画面口座番号入力→預金払出画面氏名入力→・・・→預金払出画面登録ボタン押下→預金払出画面登録ボタン押下→預金払出画面確認ボタン押下
：	：

【図３】

操作者ID	操作日時	操作画面	入力項目	入力内容	キー入力時間
AAA	2000-1-1 10:00:00	預金払出	-	入力ボタン押下	-
AAA	2000-1-1 10:01:35	預金払出	口座番号	0123456	0.5秒
AAA	2000-1-1 10:02:10	預金払出	氏名	特許　太郎	0.3秒
AAA	2000-1-1 10:02:30	預金払出	性別	男	0.4秒
AAA	2000-1-1 10:03:55	預金払出	年齢	50	0.5秒
AAA	2000-1-1 10:04:20	預金払出	払出額	100,000	0.5秒
AAA	2000-1-1 10:04:32	預金払出	-	登録ボタン押下	-
AAA	2000-1-1 10:05:00	預金払出	-	確認ボタン押下	-
AAA	2000-1-1 10:06:00	預金払出	-	戻るボタン押下	-
AAA	2000-1-1 12:35:00	預金受入	-	入力ボタン押下	-
AAA	2000-1-1 12:35:20	預金受入	口座番号	99999999	0.6秒
AAA	2000-1-1 12:35:36	預金受入	氏名	特許　花子	0.4秒
AAA	2000-1-1 12:35:58	預金受入	性別	女	0.4秒
AAA	2000-1-1 12:36:15	預金受入	年齢	20	0.5秒
AAA	2000-1-1 12:36:40	預金受入	受入額	50,000	0.3秒
AAA	2000-1-1 12:37:11	預金受入	-	登録ボタン押下	-
AAA	2000-1-1 12:38:00	預金受入	-	確認ボタン押下	-
AAA	2000-1-1 12:38:12	預金受入	-	戻るボタン押下	-
BBB	2000-1-2 15:20:38	預金払出	-	入力ボタン押下	-
BBB	2000-1-2 15:20:55	預金払出	口座番号	0123456	1.2秒
BBB	2000-1-2 15:21:35	預金払出	氏名	特許　太郎	1.1秒
BBB	2000-1-2 15:21:49	預金払出	性別	男	1.0秒
BBB	2000-1-2 15:22:00	預金払出	年齢	50	0.8秒
BBB	2000-1-2 15:22:10	預金払出	払出額	10,000	1.2秒
BBB	2000-1-2 15:22:42	預金払出	-	登録ボタン押下	-
BBB	2000-1-2 15:22:51	預金払出	-	確認ボタン押下	-
BBB	2000-1-2 15:22:07	預金払出	-	戻るボタン押下	-
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図７】



【図８】